联合的 F-FCSR 密钥流生成器

潘 臻,唐小虎
(西南交通大学信息科学与技术学院,四川成都 610031)

摘 要: 在分析带进位反馈移位寄存器(FCSR)的滤波密钥流生成器族 F-FCSR 线性弱点和其硬件方案 F-FCSR-Hv2 被攻破原因基础之上,提出了利用两个 F-FCSR 输出简单非线性运算而成的联合的 F-FCSR 密钥流生成器.该生成器避免了利用该种情况而进行的 Hell-Johansson 攻击,其生成序列通过了美国技术与标准局(NIST)STS 的 16 项随机性测试,有高的复杂度,且能抵抗相关攻击和代数攻击.

关键词: 带进位的反馈移位寄存器; 滤波生成器; 密钥流生成器; 随机性
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2010) 11-2675-05

Combined F-FCSR Key Stream Generator

PAN Zhen, TANG Xiao-hu
(*School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*)

Abstract: Based on the investigation of Feedback shift registers with carry operation (FCSR) and F-FCSR-Hv2 key stream generator which was a hardware candidate for eSTREAM, we present a generator named Combined F-FCSR. The random property of Combined F-FCSR is as good as F-FCSR and the key stream sequence passes the test of NIST's suit STS. By means of simple nonlinear operation, the Combined F-FCSR can resist the Hell-Johansson attack based on the fact that the main register of FCSR automat is linearly shifted at some special situations.

Key words: feedback shift registers with carry operation; fitered generator; key-stream generator; psedo-randomness

1 引言

线性反馈移位寄存器(LFSR)在近几十年都是构造密钥流生成器的最常用工具,特别是极大周期 LFSR 序列(m-序列)具有易于实现,生成速度快和统计特性好等优点,且理论完善,便于研究,因此作为核心部件广泛用构造密钥流生成器.但是 m-序列线性复杂度极小,利用其输出序列,B-M 算法可以很容易地将其还原出来.设计者必须利用非线性组合、非线性滤波、钟控等方式来破坏 m-序列的线性性质[1~3],以抵抗 B-M 算法的攻击.

而在 1993 年,Klapper 和 Goresky 提出了带进位的反馈移位寄存器(FCSR)[4].该生成器同样易于实现,序列生成速度快,其极大周期序列(l-序列)也具有良好统计特性,同时利用带进位加,使得 l-序列本身线性复杂度极高[4~7],可以抵抗 B-M 算法攻击,从而受到研究者的高度重视.但是 FCSR 基于 2-adic 理论,其 2-adic 复杂度极小,利用有理数逼近算法[6,8]可以很容易将 FCSR 结构还原,故 FCSR 也不能单独作为密钥流生成器.所以在 2005 年,Berger 和 Arnault 提出了利用 FCSR 主寄存器的滤波方案[9],同年在 eSTREAM 项目上提出了 F-FCSR 密钥流生成器族.该生成器族具有序列生成速度快、统计特性好、线性复杂度高的特点,其硬件方案 F-FCSR-Hv2[10]最后通过了 eSTREAM 的评选,成为 4 个硬件方案之一.不幸的是,2008 年 Hell 和 Johansson[11]以很小的代价攻破了 F-FCSR-Hv2,主要原因在于 Galois 表示的 FCSR 主寄存器在运行中会出现短暂线性情况,而 F-FCSR-Hv2 方案使用线性滤波函数,攻击者可以列出足够多的线性方程从而还原 F-FCSR-Hv2 中 FCSR 的主寄存器值.

对于密钥流生成器来说,极高的生成速度、简单的实现方式、良好的统计特性是至关重要的.由于 F-FCSR 流密码族当前只有一种有效攻击手段[11],对该密钥流生成器族的改进,使之在保证其它良好性质的前提下,避免 Hell-Johansson 攻击将具有很好的意义.本文提出联合的 F-FCSR 密钥流生成器方案,利用两个 F-FCSR 的滤波输出进行简单的非线性运算,使其在保持原有 F-FCSR 密钥流生成器族良好统计特性和速度优势的基础上,避免了文献[11]中的攻击和其它攻击,成功的改进了 F-FCSR 方案.

收稿日期:2009-07-10;修回日期:2010-05-18
基金项目:全国优秀博士学位论文作者专项资金资助项目(No.200341)

2 FCSR 自动机

令 q 为一奇负整数,满足 $2^n < -q < 2^{n+1}$,则 $d=(1-q)/2$ 为一正整数,记它的二进制展开为 $d=\sum_{i=0}^{n-1} d_i 2^i$(其中 $d_{n-1}=1$).用 $I=\{i:0\leqslant i\leqslant n-2, d_i=1\}$表示 d 除去 $n-1$ 位上所有其它的支撑.为方便起见,按照增序重排 I 中元素,即 $I=\{i_1,\cdots,i_l\}$,其中 $i_j<i_{j+1}$, $\forall j\in\{1,2,\cdots,l-1\}$.

则以 q 为连接数的 FCSR 自动机由如下两组寄存器构成:

(1)主寄存器 $\boldsymbol{M}$,由 n 个单元构成,每个单元表示为 $m_i(0\leqslant i\leqslant n-1)$.

(2)进位寄存器 $\boldsymbol{C}$,由 l 个单元构成,每个单元表示为 $c_{i_j}(0\leqslant j\leqslant l)$.

为了表示方便,我们也可以认为进位寄存器 $\boldsymbol{C}$ 包含 $n-1$ 个单元 $c_i(0\leqslant i\leqslant n-2)$,其中当 $d_i=0$ 时有 $c_i=0$,不过,此时 FCSR 寄存器真实的数目仍为 $n+l$.

寄存器在时间 t 时的转移函数在单元级上表示如下:

$$m_i(t+1)=m_{i+1}(t)\oplus d_i c_i(t)\oplus d_i m_0(t),0\leqslant i<n \quad (1)$$

$$c_i(t+1)=d_i\cdot(m_{i+1}(t)c_i(t)\oplus c_i(t)m_0(t)\oplus m_0(t)m_{i+1}(t)),0\leqslant i<n-1 \quad (2)$$

其中⊕表示异或,为方便表示,令 $m_n(t)=m_0(t)$.图 1 为 FCSR 的 Galois 结构:

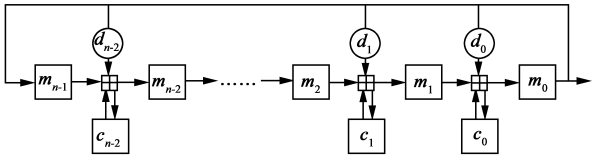

图1 带进位的反馈移位寄存器的Galois结构

其中⊞表示带进位加.进位单元与 d 二进制展开中 1 的位置对应.

主寄存器第 i 个单元在 $t\geqslant 0$ 时刻后的值构成的序列表示为 $M_i(t)=(m_i(t+\tau))_{\tau\geqslant 0}$,其中 $0\leqslant i\leqslant n-1$.当序列从时刻 $t=0$ 开始时,记为 $M_i=M_i(0)$,而 FCSR 的生成序列 M 即为 M_0.文献[9]证明 FCSR 主寄存器生成序列与 FCSR 序列具有相同的连接数和周期.

3 F-FCSR 密钥流生成器的结构及 Hell-Johansson 攻击

本节首先介绍 F-FCSR 密钥流生成,并在此基础上分析 Hell-Johansson 攻击.

F-FCSR 密钥流生成器由 FCSR 自动机与滤波函数组成,下面以 F-FCSR-Hv2(如图 2 所示)为例,介绍 F-FCSR 密钥流生成器族的具体实现.F-FCSR-Hv2 采用固定滤波函器 $F=d$,即每个进位寄存器单元后的主寄存器单元参与滤波运算.为增加吞吐量,该结构使用 $k=8$ 个不同的子滤波器.使用的 FCSR 长度(主寄存器数目)为 $n=160$,进位寄存器包含 $l=82$ 个单元.

8 个子滤波器为 $F_0,F_1,\cdots,F_7$,令向量 $\boldsymbol{F}$ 对应比特串为$(f_0,f_1,f_2,\cdots,f_{n-1})$. $\boldsymbol{F}_i$ 对应比特串为$(f_{i,0},f_{i,1},f_{i,2},\cdots,f_{i,n/k-1})$,$0\leqslant i<k$,则存在如下对应关系

$$f_{i,j}=f_{j\times k+i},0\leqslant i<k,0\leqslant j<n/k \quad (3)$$

令主寄存器向量$(m_0(t),m_8(t),m_{16}(t),\cdots,m_{152}(t))$用 $\hat{\boldsymbol{M}}_0(t)$表示,而 $\hat{\boldsymbol{M}}_i(t),1\leqslant i\leqslant 7$,表示主寄存器值$(m_i(t),m_{8+i}(t),m_{16+i}(t),\cdots,m_{152+i}(t))$. $\boldsymbol{z}(t)$为 F-FCSR-Hv2 在时刻 t 的一个字节输出,最小比特为 $z(t)_0$,最高比特为 $z(t)_7$,那么输出字节 $z(t)$可表示为

$$z(t)_i=\bigoplus_{j=0}^{19}(F_{i,j}\cdot\hat{M}_{i,j}(t)),0\leqslant i\leqslant 7 \quad (4)$$

其中 $F_{i,j}$表示向量 $\boldsymbol{F}_i$ 中的第 j 个元素,$\hat{M}_{i,j}(t)$表示 $\hat{\boldsymbol{M}}_i(t)$中的第 j 个元素.

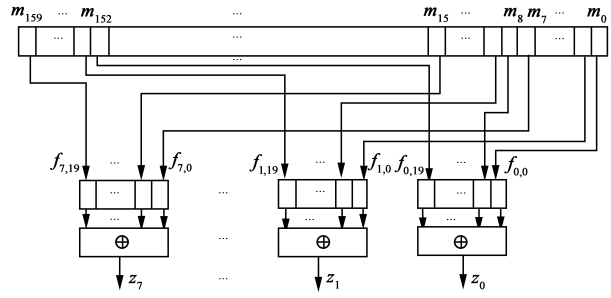

图2 F-FCSR-Hv2密钥流生成器结构图

Hell 和 Johansson[11]认为 F-FCSR 流密码族中,进位寄存器 $\boldsymbol{C}$ 变化并不是很随机是其主要弱点.原因在于它们都有一个共同的输入变量—反馈比特,当反馈比特为 0 时,$\boldsymbol{C}$ 中为 0 的单元仍为 0,为 1 的单元以 50% 的概率变为 0.所以当反馈比特连续出现多个 0 时,会将进位寄存器变为常数 0×2.设正整数,定义如下事件:

$$\mathrm{Et}(r):\boldsymbol{C}(t)=\boldsymbol{C}(t+1)=\cdots=\boldsymbol{C}(t+r)=(0,0,\cdots,0,1,0)$$

对于 F-FCSR-Hv2 而言,当 Et(r)发生时,主寄存器将出现线性平移的情况,具体如下:

$$m_i(t+r)=\begin{cases} m_i(t), & 0\leqslant i<2 \\ m_{i+\tau}(t), & 2\leqslant i<n-\tau \\ m_{i+\tau+2-n}(t)\oplus 1, & n-\tau\leqslant i<n \end{cases} \quad (5)$$

结合式(4)与式(5)可发现:$z(t+\tau)_i,0\leqslant\tau\leqslant r$,仅与 $\hat{M}_{(T+i)\bmod 8}(t)$相关.那么令

$$\boldsymbol{W}_i=(z(t)_i,z(t+1)_{i-1},\cdots,z(t+\tau)_{\tau_i},\cdots,z(t+r)_{r_i,(r+r_i)\equiv i \bmod 8})$$

其中 $\tau+\tau_i\equiv i \bmod 8$ 对于任意的 $0\leqslant\tau\leqslant r,0\leqslant i\leqslant 7$.则有:

$$\boldsymbol{W}_i=\hat{\boldsymbol{M}}_i\boldsymbol{R}_i,0\leqslant i\leqslant 7$$

这里 $\boldsymbol{R}_i$ 是一个已知的 $20(r+1)$的矩阵(由滤波器 $\boldsymbol{F}$ 决定),$\hat{\boldsymbol{M}}_i=\hat{\boldsymbol{M}}_i(t)$是含 20 个未知数的行向量.这样我们分别求解这 8 个方程组,每个方程组有 20 个未知数、$r+1$ 个方程.设矩阵 $\boldsymbol{R}_i$ 的秩表示为 $\mathrm{d}(\boldsymbol{R}_i)$,若其为 20 则可直接计算出主寄存器值,否则需要猜测 $20-\mathrm{d}(\boldsymbol{R}_i)$比特.所以正确解出这 160 个未知数的概率为:

$$\mathrm{pr}(r)=\prod_{i=0}^{7}2^{-(20-\mathrm{d}(R_i))},\mathrm{d}(R_i)\leqslant 20$$

而 $\mathrm{Et}(r)$的出现条件为:需要 $\log_2 l/2\approx 6$ 个反馈 0 使得 $\boldsymbol{C}$ 在时刻 t 变为汉明重量为 1 的常数,并需要 r 个反馈 0 使得 $\boldsymbol{C}$ 再保持为常数 r 次,则发生概率为 $p=2^{-(r+\log_2 l/2)}$,那么,一次试验解出 FCSR 主寄存器值的概率为:

$$P(r)=2^{-(r+6)}\cdot\prod_{i=0}^{7}2^{-(20-\mathrm{d}(R_i))}\leqslant 2^{-(r+6)}$$
$$\cdot\prod_{i=0}^{7}2^{-(20-r-1)}=2^{-158+7r},r\leqslant 19$$

成功攻击 F-FCSR-Hv2 的概率上限为 2^{-25}.事实上由于反馈比特的作用,在求解方程前我们可以事先确定 $r+2$ 个比特值如下:

$$m_i(t)=\begin{cases}0, & 0\leqslant i<2\\ 1, & 2\leqslant i<r+2\end{cases}\qquad(6)$$

这样可以将成功的概率提高到 2^{-23}.真实情况下成功概率会比理想状态低一些,文献[11]给出的成功概率为 $2^{-24.7}$.

4　联合的 F-FCSR 密钥流生成器

由前面叙述可知,单纯对 Galois 表示的 FCSR 主寄存器进行线性滤波将是不合适的,而使用非线性度很高的滤波器进行滤波将使得性质难于分析.所以本文提出联合的 F-FCSR 密钥流生成器,利用两个 F-FCSR 输出进行简单非线性组合,既保证了生成密钥流的统计特性,也避免了利用 FCSR 运行时可能出现短暂线性变化而进行的攻击.

下面介绍联合的 F-FCSR 密钥流生成器,该生成器密钥长度 128 比特,初始化值 $\boldsymbol{V}$ 长度 128 比特.结构如图 3 所示,使用两个不同的 F-FCSR,F_a 和 F_b,由于需要保证 128 比特安全性,主寄存器级数都为 128 级,连接数分别为 q_a,q_b,$q_a\neq q_b$,在 t 时刻 F_a 和 F_b 都输出 16 比特,滤波器为固定值,分别为 $F_a=(|q_a|+1)/2$ 和 $F_b=(|q_b|+1)/2$,按式(3),取 $k=16$,得 16 个子滤波器 $\boldsymbol{F}_{a_i}$,$\boldsymbol{F}_{b_i},0\leqslant i<16$;令 F_a 的主寄存器向量$(m_{a_i}(t),m_{a_{16+i}}(t),\cdots,m_{a_{112+i}}(t))$为 $\hat{\boldsymbol{M}}_{\boldsymbol{a}_i}(t),0\leqslant i<16$,$F_b$ 主寄存器向量$(m_{b_i}(t),m_{b_{16+i}}(t),\cdots,m_{b_{112+i}}(t))$为 $\hat{\boldsymbol{M}}_{\boldsymbol{b}_i}(t),0\leqslant i<16$,由滤波运算:

$$a(t)_i=\bigoplus_{j=0}^{8}F_{a_{i,j}}\cdot\hat{M}_{a_{i,j}}(t),0\leqslant i<16,$$
$$b(t)_i=\bigoplus_{j=0}^{8}F_{b_{i,j}}\cdot\hat{M}_{b_{i,j}}(t),0\leqslant i<16$$

得到滤波输出为 $a(t)_0,a(t)_1,\cdots,a(t)_{15}$和 $b(t)_0,b(t)_1,\cdots,b(t)_{15}$,其中 $F_{a_{i,j}}$和 $F_{b_{i,j}}$表示滤波器 $\boldsymbol{F}_{a_i}$和 $\boldsymbol{F}_{b_i}$的第 j 个值,$\hat{M}_{a_{i,j}}(t)$和 $\hat{M}_{b_{i,j}}(t)$表示主寄存器 $\hat{\boldsymbol{M}}_{\boldsymbol{a}_i}(t)$和 $\hat{\boldsymbol{M}}_{\boldsymbol{b}_i}(t)$的第 j 个值.再按如下运算式

$$s(t)_i=a(t)_i b(t)_i\oplus a(t)_{i+8}\oplus b(t)_{i+8},0\leqslant i\leqslant 7\qquad(7)$$

得到 $\boldsymbol{s}(t),s(t)_0,s(t)_1,\cdots,s(t)_7$ 表示对应比特,则由 $s(t)_{t\geqslant 0}$构成的序列即为联合密钥流生成器产生的密钥流序列.

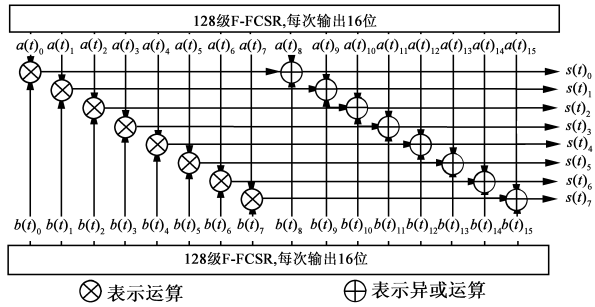

图3　联合的F-FCSR密钥流生成器

联合的 F-FCSR 密钥流生成器的"Key + IV"设置过程:输入长度皆为 128 的密钥 $\boldsymbol{K}$ 和 $\boldsymbol{V}$,$\boldsymbol{K}_L$ 为密钥的低 64 位,$\boldsymbol{K}_H$ 为密钥的高 64 位;$\boldsymbol{V}_L$ 为 $\boldsymbol{V}$ 的低 64 位,$\boldsymbol{V}_H$ 为 $\boldsymbol{V}$ 的高 64 位,约定高位在左.

(1)将 F_a 和 F_b 的主寄存器 $\boldsymbol{M}_a$,$\boldsymbol{M}_b$ 用密钥 $\boldsymbol{K}$ 和 $\boldsymbol{V}$ 初始化:

$$\boldsymbol{M}_a:=\boldsymbol{K}_L+2^{64}\boldsymbol{V}_L=(\boldsymbol{V}_L\parallel\boldsymbol{K}_L)$$
$$\boldsymbol{M}_b:=\boldsymbol{K}_H+2^{64}\boldsymbol{V}_H=(\boldsymbol{V}_H\parallel\boldsymbol{K}_H)$$

(2)将 F_a 和 F_b 进位寄存器 $\boldsymbol{C}_a$,$\boldsymbol{C}_b$ 都初始化为 0:

$$\boldsymbol{C}_a:=0,\boldsymbol{C}_b:=0$$

(3)运行 32 次,每次运行得到一个字节输出 $\boldsymbol{S}_i(0\leqslant i\leqslant 31)$;

(4)用得到的这些字节重新初始化主寄存器:

$$\boldsymbol{M}_a:=\sum_{i=0}^{15}\boldsymbol{S}_i\cdot 256^i=(\boldsymbol{S}_{15}\parallel\cdots\parallel\boldsymbol{S}_1\parallel\boldsymbol{S}_0)$$
$$\boldsymbol{M}_b:=\sum_{i=0}^{15}\boldsymbol{S}_{i+16}\cdot 256^i=(\boldsymbol{S}_{31}\parallel\cdots\parallel\boldsymbol{S}_{17}\parallel\boldsymbol{S}_{16})$$

(5)将进位寄存器重新初始化为 0:$\boldsymbol{C}_a:=0$,$\boldsymbol{C}_b:=0$;

(6)将 FCSR 运行 132 个时钟(将这一步的输出丢弃).

本方案中,选取强 2-素数 q_a,q_b 为 F_a 和 F_b 的连接数,其值如下:

$q_a=-0\mathrm{x}199\mathrm{B}63\mathrm{C}90\mathrm{F}4\mathrm{DE}193\mathrm{F}1\mathrm{FC}89\mathrm{DFCD}2\mathrm{C}484\mathrm{BB}$

$q_b=-0\mathrm{x}1\mathrm{AC}913013\mathrm{BC}417\mathrm{DFF}5\mathrm{FD}97\mathrm{CF}6\mathrm{D}318\mathrm{A}26\mathrm{B}$

且 $2^{128} < -q_a, -q_b < 2^{129}$, $l_a = 69, l_b = 70$. F_a 和 F_b 的生成序列为极大周期序列,周期分别为 $|q_a| - 1$ 和 $|q_b| - 1$.

5 联合 F-FCSR 密钥流生成器抗 Hell-Johansson 攻击的分析

对联合的 F-FCSR 密钥流生成器定义如下事件:

$\mathrm{Ed}(r)$:

$$\begin{cases} \boldsymbol{C}_{a(t)} = \boldsymbol{C}_{a(t+1)} = \cdots = \boldsymbol{C}_{a(t+r)} = (0,0,\cdots,0,1,0) \\ \boldsymbol{C}_{b(t)} = \boldsymbol{C}_{b(t+1)} = \cdots = \boldsymbol{C}_{b(t+r)} = (0,0,\cdots,0,1,0) \end{cases}$$

则在事件 $\mathrm{Ed}(r)$ 发生时,两个 FCSR 主寄存器变化情况由式(5)确定,那么就可以列出 $8(r+1)$ 个方程,由方程数 $8(r+1) \leqslant 256$ 可得整数 $r \leqslant 31$,其中输入变量线性相关.

要解方程组,需要将方程变为线性方程,可以采用的方法为:对输出比特值进行猜测,以便通过更改输出比特,将方程变为线性方程.由式(7)可知,若 $a_i(t)b_i(t) = 0, 0 \leqslant i < 8$,可得方程 $s_i(t) = a_{i+8}(t) \oplus b_{i+8}(t)$ 为线性方程;若 $a_i(t)b_i(t) = 1$,则 $s_i(t) \oplus 1 = a_{i+8}(t) \oplus b_{i+8}(t)$ 为线性方程.关键在于猜测出何时 $s_i(t)$ 取反,以获得线性方程.根据文献[9],我们可以认为 F-FCSR 的输出序列 $a_i(t)$ 和 $b_i(t)$ 随机均匀分布,那么 $a_i(t)b_i(t)$ 为 1 的概率为 1/4.则对滤波输出比特 $s_i(t)$,有 1/4 概率需要取反,以便得到线性方程,因此 8 个方程猜对的概率为 1/28,对于 $8(r+1)$ 个方程猜对的概率为 $(1/28)^{r+1} \approx 2^{-4.8(r+1)}$.

$\mathrm{Ed}(r)$ 发生概率为 $\mathrm{Et}(r)$ 的平方,即 $2^{-2(r+\log_2 l/2)} = 2^{-2(r+6)}$.令方程组秩为 n',那么正确还原出主寄存器值的概率为:

$$P(r) = 2^{-2(r+6)} \cdot 2^{-4.8(r+1)} \cdot 2^{-(n-n')} \leqslant 2^{-6.8(r+1)-10} \cdot 2^{-(256-8(r+1))} = 2^{1.2r-264.8}, r \leqslant 31$$

攻击成功概率上界为 $2^{-227.6}$.根据式(6)可以事先确定 $2(r+1)$ 个变量,则有:

$$P(r) = \leqslant 2^{-6.8(r+1)-10} \cdot 2^{-(256-2(r+2)-8(r+1))} = 2^{3.2r-260.8}, r \leqslant 24$$

$r \leqslant 24$ 是由 $(256 - 2(r+2) - 8(r+1)) \geqslant 0$ 确定,此时攻击成功概率上界为 2^{-184},所以该攻击对联合的 F-FCSR 流密码发生器无效.

6 联合的 F-FCSR 密钥流生成器的其他密码分析

美国国家技术与标准局 NIST 推出的 STS 软件包[12]是当前伪随机性测试中最具权威性的测试工具.本文利用 STS 统计测试软件(版本 1.6)分别对 F-FCSR 流密码族中的 F-FCSR-8 和联合的 F-FCSR 的生成序列进行了测试.经过对 1000 组长度为比特的生成序列进行测试,结果显示两种密钥流生成器的生成序列通过率都在 99%左右,其通过率偏差在 1%之内,见图 4.所以我们认为联合的 F-FCSR 密钥流生成器生成的密钥流具有良好的统计特性.

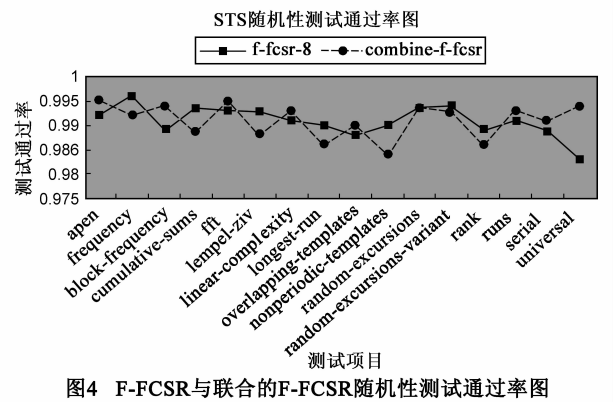

图4 F-FCSR与联合的F-FCSR随机性测试通过率图

类似于文献[9]的分析,可得联合的 F-FCSR 密钥流生成器生成序列在复杂度上与随机序列近似,同时也能够抵抗相关攻击和代数攻击.

7 结论

本文分析了基于带进位的反馈移位寄存器(FCSR)滤波的密钥流生成器方案(F-FCSR).研究了 F-FCSR 的线性弱点,在充分分析了 F-FCSR-Hv2 被攻破的原因的基础之上,提出了联合的 F-FCSR 密钥流生成器.给出了参数,设计了初始化过程.该密钥流生成器利用两个线性 F-FCSR 输出序列进行简单非线性运算,使得利用 FCSR 出现线性平移而进行的 Hell-Johansson 攻击无效.其生成序列通过了美国技术与标准局(NIST)的 STS 软件包的 16 项随机性测试且能抵抗相关攻击和代数攻击.结果表明改进后的方案弥补了 F-FCSR 方案的缺陷,却保证了原有的良好性质,生成简单,速度快,统计特性良好.所以认为联合的 F-FCSR 流密码生成器是成功的.

参考文献:

[1] 丁存生,肖国镇.流密码学及其应用[M].北京:国防工业出版社.1994.

[2] 冯登国,裴定一.密码学导引[M].北京:科学出版社.1999.

[3] 张木想,肖国镇.流密码中非线性组合函数的分析与设计[J].电子学报,1996,24(1):48 - 52.
ZHANG Mu-xiang, XIAO Guo-zhen. analysis and design of nonlinear combining function in stream ciphers[J]. Acta Electronica Sinica, 1996, 24(1): 48 - 52. (in Chinese)

[4] Klapper A, Goresky M. 2-Adic shift register[A]. Fast Software Encryption [C]. Combridge, U.K.: Springer-Verlag, 1993. 174 - 178.

[5] Goresky M, Klapper A. Feedback register based on ramified ex-

tensions of the 2-adic number[A]. Advances in Cryptology-Eurocrypt'94[C]. Perugia, Italy: Springer-verlag 1994. 215 – 222.

[6] Klapper A, Goresky M. Feedback shift registers, 2-adic span and combiners with memory[J]. Journal of Cryptology, 1997, 10(1): 111 – 147.

[7] Goresky M, Klapper A. Fibonacci and galois representations of feedback-with-carry shift registers[J]. IEEE Transactions on Information Theory, 2002, 48(11): 2826 – 2836.

[8] Arnault F, Berger T P, Necer A. Feedback with carry shift registers synthesis with the euclidean algorithm[J]. IEEE Transactions on Infromation Theory, 2005, 50(5): 910 – 917.

[9] Arnault F, Berger T P. Design and properties of a new pseudorandom generator based on a filtered FCSR automaton[J]. IEEE Transactions on Computers, 2005, 54(11): 1374 – 1383.

[10] Arnault F, Berger T P, Lauradoux C. Update on F-FCSR Stream Cipher[DB/OL]. http://www.ecrypt.eu.org/stream/, 2008-4-2.

[11] Hell M, Johansson T. Breaking the F-FCSR-H stream cipher in real time[A]. Advances in Cryptology-ASIACRYPT 2008[C]. Melbourne, Australia: Springer-Verlag, 2008. 557 – 569.

[12] Rukhin A, Soto J, Nechvatal J, et al. A Statistical Test Suite for Random and Pseudorandom Number Generator for Cryptographic Applications[DB/OL]. NIST Special Publication 800-22, http://csrc.nist.gov/rng/SP800-22b.pdf. 2004-05-01.

作者简介:

潘　臻　男, 1981 年 4 月生于四川内江, 2007 年进入西南交通大学攻读博士学位, 主要研究方向为流密码分析与设计、流密码应用和 RFID 等.

E-mail: zpan5@163.com

唐小虎　男, 博士, 1972 年 3 月生于四川绵竹, 现任西南交通大学信息学院教授、博士生导师. 主要研究方向为信息论与编码理论、网络信息安全等.

E-mail: xhutang@ieee.org